OFFICE OF THE CHIEF INFORMATION OFFICER (CAJR)

The mission of the Office of the Chief Information Officer (OCIO) is to administer the Centers for Disease Control and Prevention's (CDC) information resources and information technology programs including collection, management, use, and disposition of data and information assets; development, acquisition, operation, maintenance, and retirement of information systems and information technologies; IT capital planning; enterprise architecture; information security; education, training, and workforce development in information and IT disciplines; development and oversight of information and IT policies, standards, and guidance; and administration of certain other general management functions and services for CDC. (Approved 9/28/2019; Effective 10/4/2019)

Office of the Director (CAJR1)

(1) Provides leadership, direction, coordination, support and assistance to CDC's programs and activities to enhance CDC's strategic position in public health informatics, information technology, and other information areas to optimize operational effectiveness (2) represents CDC with various external stakeholders, collaborators, service providers, and oversight organizations; (3) maintains liaison with HHS officials; (4) directs the strategic objectives and operations of offices within the OCIO to ensure effective and efficient service delivery; (5) provides strategic and tactical management of CDC's IT investments and initiatives; (6) delivers change management support to promote the adoption of technology solutions and process improvements; (7) manages and ensures proper execution of enterprise projects and programs; (8) directs IT research and development priorities; (9) leads, plans, and manages CDC's information technology (IT) budget development and review processes; (10) plans and directs the Capital Planning Investment Control processes; (11) develops and monitors earned value management (EVM) analyses of project cost, schedule and deliverable commitments; (12) provides guidance to program and project managers on the use of tools for preparing investment documentation that meet CDC, HHS, and OMB requirements; (13) provides guidance to program and project managers on Technology Business Management; and (14) supports CDC information resource governance structures. (Approved 9/28/2019; Effective 10/4/2019)

Office of Business Operations (CAJR16)

(1) provides leadership, oversight, and guidance for OCIO's centralized accounting, acquisition and budget services; (2) provides guidance, oversight, and coordination of OCIOs organizational design and human capital management; (3) provide OCIO IT policy coordination; (4) provides expertise in interpreting applicable laws, regulations, policies, and offers guidance, direction, and coordination in resolving issues; (5) advises and assists the CDC Chief Information Officer, OCIO office directors, and senior staff on all matters regarding internal business service operations; (6) maintains internal controls; (7) provides leadership and strategic support in the determination of long-term operational needs; (8) provides collaboration and centralized consolidation of office reporting requirements; (9) provides strategic planning and coordination of OCIO transformation projects and initiatives; (10) provides leadership, oversight, and guidance for OCIO enterprise risk management, continual process improvement; performance measures and evaluation (11) provides and oversees the delivery of OCIO-wide administrative management and support services in the areas of fiscal management, personnel, travel, records management, vendor management, internal controls, and other administrative services; (12) plans, develops, manages and conducts oversight of OCIOs information technology and services

contracts; and (13) provides coordination and oversight for internal and external OCIO communications. (Approved 9/28/2019; Effective 10/4/2019)

Enterprise Data Office (CAJR17)

(1) Develops, promotes, implements, and evaluates data science approaches for improved research of large and complex data sets; (2) maintains and leverages data acquired from multiple sources; (3) develops and implements solutions to strengthen information systems and reporting; (4) develops and implements computer-based decision support tools and mobile applications; (5) collaborates with other CDC programs to develop and promote informatics solutions for improving data management, practice, and preparedness; (6) identifies needs and develops strategies and approaches to acquire and manage enterprise statistical software licenses; (7) develops internal cost allocation methods and coordinates allocation of costs for annual license renewal payments; and (8) coordinates and manages an enterprise data governance program and procedures to maintain "fit for purpose" standards and decision rights for enterprise data. (Approved 9/28/2019; Effective 10/4/2019)

Customer Engagement Office, (CAJRH)

The Customer Engagement Office oversees agency-wide OCIO customer relationships, account management, innovation and research and development agenda for business and administrative systems. (Approved 9/28/2019; Effective 10/4/2019)

Office of the Director (CAJRH1)

(1) Provides account management representing the entire range of OCIO products and services to OCIO customers; (2) maintains and expands OCIO customer relationships; (3) manages OCIO help desk response, coordination, tracking and reporting; (4) provides and maintains end user support services for OCIO products and devices; (5) collaborates with OCIO offices and customers in support of IT innovation and to achieve program outcomes; and (6) ensures the execution of OCIO's research and development agenda. (Approved 9/28/2019; Effective 10/4/2019)

Program Services Branch (CAJRHB)

(1) Focuses on improving the end-to-end experience of OCIO customers and fostering a customer-first mentality by serving as the day-to-day point of contact; (2) works with other OCIO units to better understand technology users' experiences and to align OCIO products and services to customer needs; (3) creates customer interview and survey guides, journey maps, and personas; (4) develops and strengthens OCIO's customer experience abilities and processes by helping teams adapt to shifting customer preferences; (5) applies research strategies and outputs to shed light on customer perspectives and collect customer feedback; and (6) coordinates solution development efforts to address customer needs. (Approved 9/28/2019; Effective 10/4/2019)

Customer Assistance Branch (CAJRHC)

(1) Serves as the first line of help when customers encounter problems or defects with products and programs; (2) provides end user services support including installs, moves, adds and changes, and desk-side support; (3) manages and coordinates product, service, systems and infrastructure help desk; (4) answers and addresses customer problems directly; (5) escalates customer problems and questions to

appropriate OCIO office or branch staff and tracks open help desk tickets to resolution; (6) provides meeting support services including electronic meeting systems; and (7) manages, conducts, and monitors OCIO supported device deployment and refresh activities. (Approved 9/28/2019; Effective 10/4/2019)

Emerging Technology & Design Acceleration Branch (CAJRHD)

(1) Collaborates with CDC programs and external partners to develop innovative technologies and techniques to positively impact public health practice; (2) executes OCIO's research and development agenda in support of advancing public health programs and enterprise IT; (3) prototypes products and processes and gathers user feedback to evaluate and refine big ideas to prioritize investments; (4) develops, implements and maintains OCIO's intake process for new mission-based technology requests; (5) transitions new technology-based solutions, standards, and techniques to programs for deployment and implementation; (6) provides consultation, evaluation, guidance, and support in the use of new informatics solutions and architecture; (7) works directly with customers to facilitate design sessions that integrate human-centered design principles; (8) rapidly defines problems, facilitates design sessions, creates prototypes, conducts pilot projects, and examines and tests hypotheses to support information technology solutions; and (9) participates and represents the agency on technology innovation committees, workgroups, organizations, and councils, within CDC and with other federal agencies. (Approved 9/28/2019; Effective 10/4/2019)

Digital Services Office (CAJRJ)

The Digital Services Office (DSO) oversees agency-wide business and administrative customer facing information technology solutions and OCIO's modernization roadmap. (Approved 9/28/2019; Effective 10/4/2019)

Office of the Director (CAJRJ1)

(1) Manages and approves new product development and deployments for all customer facing solutions; (2) executes the OCIO modernization strategy and roadmap, and ensures adequate resources are available to achieve the organization's strategic goals and objectives; (3) provides approval for and ensures the execution of OCIO product lifecycle roadmaps; (4) facilitates cross-functional collaboration across OCIO to achieve targeted performance goals and business outcomes; (5) provides identity and access management services to meet current and future organizational needs; (6) ensures efficient operations and proper maintenance of all network, security, storage and computer systems; (7) works with the Cybersecurity Program Offices to address identified application, system, network and infrastructure performance issues; (8) ensures the availability of a modern, customer-driven IT workforce within DSO; and (9) coordinates, tracks, and manages project assignments for all DSO human and technology resources. (Approved 9/28/2019; Effective 10/4/2019)

Technology Solutions Branch (CAJRJB)

(1) Identifies, tests and integrates new technologies and digital services; (2) ensures products and services align to customer needs and meet OCIO's modernization and transformation strategic objectives; (3) standardizes and enhances technology and service development practices; (4) obtains and manages cloud computing services from cloud service providers; (5) designs, deploys and maintains Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) such as virtual machines, networks and databases; (6) identifies optimization opportunities and coordinates

technology modernization efforts; and (7) operates and maintains business and mission systems, including change requests, release cycle management, and decommissioning of redundant or outdated technology. (Approved 9/28/2019; Effective 10/4/2019)

Product Management Branch (CAJRJC)

(1) Manages the vision and strategy for OCIO products and ensures alignment to customer needs and modernization goals; (2) works across OCIO service teams as well as with other OCIO offices and customers to define current and future product capabilities and requirements; (3) establishes and maintains product lifecycle roadmaps; (4) coordinates cross-service and cross-product collaboration; (5) maintains all network, security, storage and computer systems to support global mission activities; (6) detects and responds to global incidents that affect network performance and availability; (7) develops and maintains backup and recovery processes to enable global IT services, and global help desk support capabilities; and (8) collaborates with partners to implement country-specific IT regulations and requirements. (Approved 9/28/2019; Effective 10/4/2019)

Identity and Access Management Branch (CAJRJD)

(1) Develops and maintains CDC's identity and access management (IAM) strategy; (2) designs and deploys identification standards for federal employees, contractors and external partners; (3) designs, implements and deploys IAM services; (4) performs identity attribute management; and (5) manages identity governance for the enterprise. (Approved 9/28/2019; Effective 10/4/2019)

Infrastructure Services Branch (CAJRJE)

(1) Maintains and monitors all IT infrastructure for network, security, data centers, storage, telecommunications, and computer systems; (2) works with the Cybersecurity Program Office to detect and respond to incidents that affect network performance and availability, and security of information assets; (3) coordinates approved changes and upgrades to the CDC infrastructure environment; (4) develops and maintains backup and recovery processes to maintain continuity of operations; and (5) collaborates with Customer Engagement Office to facilitate appropriate help desk support capabilities. (Approved 9/28/2019; Effective 10/4/2019)

Cybersecurity Program Office (CAJRK)

The Cybersecurity Program Office oversees agency-wide cyber functions, privacy, risk management, threat protection, and compliance to ensure the safety of CDC's public health mission. (Approved 9/28/2019; Effective 10/4/2019)

Office of the Director (CAJRK1)

(1) Manages CDC privacy policies, procedures, and processes; (2) ensures compliance with Federal Information Security Management Agency (FISMA), OMB, HHS, CDC and other government mandates, and regulations; (3) establishes and oversees CDC information security risk management and compliance activities; (4) provides and manages a centralized network and security operations command and control center; (5) provides oversight and implementation of Information Security Continuous Monitoring (ISCM) activities, including maintenance of the agency's Continuous Diagnostics and Mitigation (CDM) program; (6) manages CDC cybersecurity related insider threat detection, response,

and security awareness training programs; (7) manages and executes privacy incident response, including compliance and remediation efforts; (8) performs Personally Identifiable Information (PII) inventory and data classification mapping; and (9) works with OCIO offices and customers to effectively implement privacy standards in support of program outcomes. (Approved 9/28/2019; Effective 10/4/2019)

Policy Branch (CAJRKB)

(1) Works with OCIO development and operations teams to identify and adapt applicable standards and service level agreements (SLAs) for OCIO products and services; (2) ensures CDC-wide compliance and adherence to applicable FISMA and other federal mandates, standards, practices and policies; (3) oversees an annual security policy review and approval process; (4) develops and manages CDC Cybersecurity policies; (5) determines security requirements for IT systems to receive an authority to operate (ATO) and connect to agency systems and networks; and (6) performs ongoing authorization of information technology systems. (Approved 9/28/2019; Effective 10/4/2019)

Risk and Compliance Branch (CAJRKC)

(1) Establishes and implements information security risk management protocols and processes; (2) performs penetration testing of all external and important systems; (3) conducts security architecture reviews of key technologies; (4) provides FISMA management, including audits of agency IT assets (architecture, hardware, software, networks, hosted applications, etc.) for possible security risks and compliance to cybersecurity standards and policies identified by the Cybersecurity Policy Branch; (5) manages corrective efforts for security weaknesses, including Plan of Action and Milestones (POA&Ms); (6) collects, synthesizes and reports on compliance to standards and cybersecurity incidents, including risks, issues, incidents, violations, and the status of remediation efforts; and (7) develops and implements cyber and information security awareness activities and training. (Approved 9/28/2019; Effective 10/4/2019)

Advanced Threat Protection Branch (CAJRKD)

(1) Administers the integrated Network Operations Center (NOC) and Security Operations Center (SOC) central command and control Systems Management Team (SMT) for monitoring, triaging, troubleshooting and escalating all detected, reported, or potential security incidents, performance issues, enterprise services and infrastructure operations; (2) oversees Computer Security Incident Response (CSIR); (3) monitors network, systems, infrastructure, and application security; (4) establishes network defenses through proactive and reactive measures; (5) identifies and mitigates network intrusion attempts; (6) investigates security policy violations and other cybersecurity-related anomalies; (7) conducts technical and operational cybersecurity vulnerability assessments and manages remediation efforts; (8) conducts code vulnerability and penetration testing, including detailed packet analysis on triggered events and malicious code, and troubleshoots identified threats and vulnerabilities; (9) applies and coordinates directed cybersecurity compliance requirements; (10) coordinates reporting and incident response actions with DHS US-CERT, HHS CSIRC and/or other external entities; (11) provides tool management and configuration to implement, configure and maintain the capabilities and tools used to deter and detect threats, risks, and vulnerabilities on the CDC enterprise network; (12) develops, deploys and maintains security products and tools to the CDC environment; (13) deploys, configures and operates CDC enterprise firewalls; (14) designs, implements and maintains security controls, develops

and deploys continuous monitoring systems within the infrastructure environment; (15) deploys, configures and operates CDC enterprise Continuous Diagnostics & Mitigation (CDM) tools; and (16) consolidates critical IT data from disparate sources into meaningful data sets used to effectively conduct cyber Hunt activities across the enterprise. (Approved 9/28/2019; Effective 10/4/2019)

Engineering and Technologies Branch (CAJRKE)

(1) Develops and maintains security architecture and engineering procedures, policies and frameworks including firewall policy; (2) provides technical security architecture and engineering advice and expertise to OCIO development, operations and maintenance teams and particularly the Digital Services Office; (3) manages and maintains system and user access control lists (ACLs); (4) establishes policies for and maintains perimeter networks or demilitarized zones that prevent interaction between internal and external networks; and (5) conducts assessment and testing of emerging cybersecurity technologies to identify, evaluate, and make recommendations to integrate potential advances in cyber threat protection. (Approved 9/28/2019; Effective 10/4/2019)

Cyber Intelligence and Insider Threat Branch (CAJRKG)

(1) Establishes policies and procedures for detecting and responding to insider threats; (2) establishes policies and procedures for detecting and responding to intelligence threats resulting from foreign travel of CDC personnel; (3) conducts personnel forensics and analysis of anomalous cybersecurity activities, including data transiting, storage, and use of electronic media; (4) conducts self-phishing exercises and follow-up activities; (5) delivers analytic and technical support to Law Enforcement, Counterintelligence and National Security inquiries and investigations; (6) deploys and maintains systems that allow the examinations in a forensically-sound manner using repeatable and defensible processes; (7) assists in the implementation of intelligence-driven threat mitigation, including applying tools that identify and mitigate current and projected risks; and (8) ensures that insider threat related activities occur in accordance with applicable privacy laws and policies. (Approved 9/28/2019; Effective 10/4/2019)